El monitoreo de la actividad en bases de datos está evolucionando hacia la auditoría y la protección de bases de datos

22 de febrero de 2012 ID:G00230083
Analista(s): Jeffrey Wheatman

RESUMEN

Las preocupaciones sobre la seguridad de bases de datos, los requerimientos de regulación y las capacidades ampliadas de los proveedores están llevando al surgimiento de una clase de tecnologías que Gartner identifica ahora como herramientas de auditoría y protección de bases de datos. Las herramientas de monitoreo de actividad en bases de datos se están transformando en suites de auditoría y protección de bases de datos [DAP, por sus siglas en inglés].

Panorama general

La auditoría y la protección de bases de datos (DAP) representa un avance evolutivo importante con respecto a anteriores herramientas de monitoreo de actividad en bases de datos (DAM). Los gerentes de seguridad, los administradores de bases de datos (DBAs) y otros interesados, que estén preocupados con proteger datos sensibles en las bases de datos, deben evaluar estas cada vez más maduras suites.

Conclusiones clave

- Las empresas se preocupan cada vez más sobre la seguridad de las bases de datos a medida que lidian con repositorios que contienen cantidades grandes y crecientes de datos regulados o, por otras razones, sensibles o críticos.
- El mercado DAP continúa madurando, con proveedores que expanden sus ofertas y que tienen como blanco un rango más amplio de casos de uso. Sin embargo, todavía no queda claro si las empresas estarán dispuestas o serán capaces de adoptar algunas de las más avanzadas funciones de DAP.
- Muchas empresas no poseen la madurez de programas, los recursos y las aptitudes necesarios para implementar algunos de los rasgos más sofisticados de DAP que se encuentran disponibles.
- La conformidad legal y regulatoria continúa siendo la razón más común para las inversiones en DAP, y Gartner piensa que éste seguirá siendo el caso a mediano plazo.

Recomendaciones

- Implementar funcionalidad DAP para mitigar los altos niveles de riesgo que resultan de la vulnerabilidad de las bases de datos, y abordar los descubrimientos de la auditoría en áreas tales como la discriminación de tareas y la gestión de cambios de las bases de datos.
- Desarrollar una estrategia de seguridad de las bases de datos que incorpore metas y requerimientos a corto y largo plazo. Evaluar ofertas de DAP como parte de un programa de seguridad de las bases de datos.
- Considerar soluciones alternativas para las funciones de DAP en las que no se requiera una funcionalidad completa. Reconocer que la viabilidad de alternativas estará sujeta a compromisos de costo-beneficio.

Lo que necesita saber

Las empresas están, entendiblemente, cada vez más preocupadas con los riesgos asociados con su rápidamente creciente uso de sistemas de gestión de bases de datos relacionales (RDBMSs). Los auditores están observando más cercanamente cómo se controla el acceso a las grandes reservas de datos en estos sistemas, y las empresas están siendo presionadas para adoptar controles de datos más agresivos y expansivos. Las herramientas DAP pueden proveer una solución integral a los requerimientos de seguridad de las bases de datos, pero las ofertas actuales de los proveedores exceden las necesidades de aquellos que adoptan tecnología convencional. Sin embargo, hacer uso de las capacidades principales de una suite de DAP y trazar las futuras inversiones con relación al plan de acción del proveedor preparará el escenario para una futura y mejor seguridad de los datos. Las empresas que están considerando inversiones en DAP deben estar conscientes de las capacidades alternativas y complementarias de otras herramientas y proveedores de seguridad de datos.

Análisis

Descripción de la tecnología

DAP — un término que Gartner desarrolló para remplazar el anterior concepto de DAM — se refiere a las suites de herramientas que se utilizan para apoyar la identificación y reportar comportamiento inapropiado, ilegal o de otra forma indeseable en las RDBMSs, con mínimo impacto en las operaciones y la productividad del usuario. Estas suites han evolucionado de herramientas DAM — que ofrecían análisis de la actividad del usuario en las RDBMSs y alrededor de ellas— para abarcar un conjunto más integral de capacidades, que incluyen:

- Descubrimiento y clasificación.
- Gestión de vulnerabilidades.
- Análisis al nivel de aplicación.
- Prevención de intrusión.
- Soporte de seguridad de datos no estructurados.
- Integración de gestión de identidad y acceso.
- Soporte de gestión de riesgos.

Definición de la tecnología

Hoy día, las suites de DAP entregan un amplio rango de funciones construidas alrededor de las funciones esenciales de lo que previamente Gartner identificaba como tecnología DAM: recolectar, regularizar y analizar el tráfico y las actividades en las bases de datos. Gartner ha visto que las capacidades de estas suites se han extendido significativamente, particularmente durante los últimos 12 meses, con la adición de funcionalidad complementaria y periférica. Estas mejoras y extensiones en curso han dado como resultado niveles más altos de madurez del producto y mayor soporte para más casos de uso — y han expandido el mercado potencial para incluir empresas que tienen un enfoque estratégico a la seguridad de datos. Los proveedores en este mercado necesitarán expandir sus capacidades de prevención en tiempo real, posiblemente a través de las relaciones con herramientas de ocultamiento de datos dinámicos, encriptación y tokenización. El DAP provee un mayor soporte de auditoría y monitoreo que el registro interno, el cual puede añadir gastos generales significativos y no provee el mismo nivel de granularidad que las herramientas DAP. Más aún, DAP provee un soporte integral multiplataforma en ambientes heterogéneos de base de datos, y puede servir como una adición eficaz para sistemas de análisis de identidad y acceso.

Capacidades esenciales DAP

Recolección de eventos, análisis e informe

Las herramientas DAP, como otras tecnologías de monitoreo de seguridad — como las herramientas de gestión de información de seguridad y eventos (SIEM) y los sistemas de detección de intrusión — recolectan, engloban, regularizan y analizan información de un número de bases de datos y fuentes de aplicaciones diversas, y proveen un mecanismo de respuesta y flujo de trabajo (es decir, definen que debe suceder cuando ocurre un potencial incidente de seguridad).

Gestión y auditoria de la Política de Seguridad de la base de datos

La gestión centralizada es una propuesta de valor importante para las herramientas DAP en comparación con las soluciones del registro interno. Tal gestión provee la capacidad de estandarizar las normas, la configuración y la notificación a través de todas las plataformas compatibles, mientras que provee controles basados en roles para la configuración e informe para apoyar la discriminación de tareas.

Monitoreo de usuario privilegiado

Las interacciones con clientes de Gartner muestran claramente que la mayoría de las inversiones en DAP están encaminadas por la necesidad de monitorear la actividad de usuarios privilegiados. La meta principal es revisar la actividad del administrador sobre una base periódica o como sea necesaria. Una meta secundaria es llevar a cabo monitoreo y alerta en tiempo real para captar actividad administrativa inapropiada, ya sea deliberada (por ejemplo, ver datos protegidos) o accidental (por ejemplo, otorgar acceso excesivo a usuarios).

Capacidades secundarias de DAP

Prevención y bloqueo de acceso/ataques

Un caso de uso cada vez más importante es la capacidad para proveer bloqueo en tiempo real de actividad obviamente inapropiada o maliciosa. Algunos ejemplos incluyen prevenir que un DBA lea los contenidos de una tabla con números de tarjetas de crédito en ella, prevenir ataques de inyección SQL o desbordamientos del búfer, e implementar parches virtuales en casos de vulnerabilidades conocidas pero no cubiertas. El bloqueo se debe usar con gran cuidado, sin embargo, por el potencial impacto de falsos positivos.

Descubrimiento y clasificación

Las empresas frecuentemente no tienen claro cuáles RDBMSs existen en sus ambientes y qué datos se guardan en ellos. Esto puede hacer que el llevar un registro de los cambios en las bases de datos y en los datos que almacenan sea una tarea desafiante. La capacidad de las herramientas DAP para "arrastrarse a través" de la infraestructura de la empresa, descubrir bases de datos y clasificar los datos en ellas pueden ser una ayuda significativa para los esfuerzos en programas de seguridad de datos.

Vulnerabilidad y gestión de la configuración

Las herramientas de evaluación de la vulnerabilidad son una parte integral de cualquier programa de gestión de amenazas y vulnerabilidad. Muchas suites de DAP tienen capacidades de escaneo más profundas que las herramientas de gestión de la vulnerabilidad en red, incluyendo el escaneo de parches faltantes y otras malas configuraciones, así como la capacidad de comparar la configuración actual con el punto de referencia, y algunas veces con herramientas de gestión de cambios y configuración, para asegurar que los cambios sean pre-aprobados.

Auditoría y monitoreo de usuarios y aplicaciones

La capacidad para recolectar y analizar los componentes de acceso de datos del tráfico de aplicaciones es un desafío para la mayoría de las empresas. Se implementan frecuentemente IDs y conexiones compartidas al nivel de la aplicación para acelerar el funcionamiento, pero esto añade un nivel de abstracción. Una conexión compartida englobará varias solicitudes en una consulta SQL para el RDBMS; esta solicitud puede contener comandos SQL que violen una norma mezclados con comandos SQL que no lo hagan. Las herramientas DAP siguen añadiendo capacidades para mantener el contexto y mapear de vuelta comandos SQL a solicitudes de usuarios individuales.

Evaluación de usuarios y permisos

Las bases de datos mantienen sus propias reservas de identidad y normas, y, como los permisos de usuario son frecuentemente evaluados al nivel de la aplicación —en vez de en los repositorios subyacentes—, el software de gestión de identidad general de propósito no cubre bien las bases de datos. Algunos proveedores DAP pueden extraer e informar sobre estos permisos de tal forma

que equipos de seguridad, conformidad, e incluso de aplicaciones y bases de datos puedan evaluar el acceso al modelo de control.

Requerimientos de operación

DAP puede implementarse utilizando una combinación de dos arquitecturas básicas:

- **Recolectores de red:** Éstos son rápidos y centralizados y no añaden gastos a la capa de servidor, pero dejan pasar actividad como la de consola directa o remota, así como mecanismos de control de la base de datos y procedimientos almacenados.
- **Recolectores agente:** Estas pequeñas piezas de código capturan actividades locales o datos registrados y los mandan a un lugar centralizado para su recolección y análisis. Los agentes "ven" más, pero añaden gastos de servidor. Si instalar agentes locales es impráctico, entonces se puede utilizar la implantación de recolectores puramente de red.

Usos

Gartner ha identificado dos casos principales de uso de DAP:

- **El monitoreo de usuarios privilegiados** (el caso de uso más común) se enfoca en monitorear, analizar e informar sobre las acciones llevadas a cabo por usuarios (como DBAs y administradores de aplicación) con un alto nivel de acceso a datos dentro de la base de datos. DAP se usa para identificar y prevenir que los usuarios privilegiados accedan a datos, modifiquen los RDBMS, o creen o modifiquen cuentas de usuario o permisos.
- **El monitoreo de usuarios de aplicaciones** (menos común, pero cada vez más importante) se enfoca en la actividad de usuarios finales y aplicaciones que se conectan a la base de datos. El propósito de este monitoreo es detectar abusos deliberados o inadvertidos de los privilegios de acceso legítimos. Algunos auditores y equipos de seguridad están evaluando o implementando tecnologías DAP para cumplir con requerimientos contractuales y de regulación y lograr metas de gobernabilidad de datos.

Un tercer caso de uso se relaciona con atacar la detección y la prevención. Éste parece ser un tercer caso de uso principal, pero el ataque típicamente tiene como blanco comprometer las cuentas de usuarios privilegiados o el acceso al nivel de aplicación. Este caso de uso no es realmente el final de juego, sino más bien un paso intermedio que puede ser necesario antes de que se encuentren comprometidos el sistema completo o los datos.

Los requerimientos de cumplimiento de regulación — por ejemplo, los del PCI Data Security Standard [Estándar de Seguridad de Datos], la Health Insurance Portability and Accountability Act (HIPAA, Ley Federal de Portabilidad y Responsabilidad de los Seguros de Salud), y las regulaciones de privacidad globales — continúan siendo el principal impulsor para la inversión en DAP. Gartner está, sin embargo, buscando incrementar la inversión como parte de un programa de seguridad de datos.

Beneficios y riesgos

DAP no ha alcanzado todavía su potencial completo, pero representa una inversión que vale la pena para las empresas con bases de datos que contienen datos confidenciales, propiedad intelectual, o cualquier dato sujeto a requerimientos de protección legales y de regulación. Estas herramientas continuarán creciendo en madurez, funciones y facilidad de uso, y continuarán entregando beneficios como parte de un programa de seguridad de datos de la empresa. DAP puede beneficiar también a programas de gestión de riesgos. Muchas instalaciones comienzan siendo pequeñas y crecen en tamaño y complejidad con el tiempo cuando las empresas ven un valor incrementado de sus inversiones.

Alternativas de tecnología

Las herramientas SIEM pueden ser usadas para el monitoreo de las bases de datos. SIEM provee un monitoreo más amplio y, en algunos casos, soporte "suficientemente bueno" para las RDBMSs.

Las herramientas de prevención de pérdida de datos (DLP) que están al tanto del contenido pueden proveer visibilidad al acceso de datos, y pueden ser usadas como una alternativa a DAP en casos de uso centrados en los datos; sin embargo, estas herramientas no tienen conocimiento integrado de cómo "trabajan" las RDBMSs y carecen de visibilidad de actividades administrativas como la gestión de modificaciones de esquema y cuentas.

Las empresas con limitaciones financieras pueden hacer uso de auditoría y registro de RDBMS internos utilizando herramientas o secuencias de comandos de producción local. Sin embargo, este enfoque está limitado por los altos gastos de auditoría interna y la dificultad para crear soluciones de producción local en ambientes heterogéneos.

Los escaneos de vulnerabilidad de red proveen un subconjunto limitado de pruebas de RDBMS y frecuentemente son suficientes para las auditorías. Estas herramientas de escaneo frecuentemente se despliegan con el necesario conteo para manejar y responder a los descubrimientos, proveyendo de esa manera de una solución menos cara (aunque menos efectiva).

El encriptamiento, la tokenización y el ocultamiento pueden usarse para proteger los datos de accesos inapropiados, pero son insuficientes para identificar accesos inapropiados (por ejemplo, meter muchos datos muy rápido) por parte usuarios legítimos.

Las herramientas de gobernabilidad de identidad y acceso tienen un conjunto limitado de funciones que se utilizan para monitorear y analizar datos, pero carecen de la granularidad y visibilidad en ambientes estructurados de datos, y el conjunto de sus características se centra predominantemente en la aplicación.

Reglas de selección

La selección de herramientas DAP es relativamente simple, con el soporte de la plataforma tendiendo a ser la constricción más importante. Todas las herramientas DAP son compatibles con las plataformas RDBMS más comunes —Microsoft SQL Server, Oracle y DB2—, pero la compatibilidad con otras plataformas puede no ser así de consistente o comprehensiva. Los requerimientos del cliente a más largo plazo se deben ajustar al plan de acción del proveedor. Las arquitecturas flexibles provistas por la mayoría de las plataformas permiten decisiones simples, y pueden satisfacer las necesidades de la mayoría de los clientes, aunque la facilidad de uso y la escalabilidad de las implantaciones pueden variar mucho de un proveedor a otro.

Rendimiento del precio

El costo de suites de DAP es bastante constante, con una implantación al nivel de entrada que cuesta típicamente menos de $100,000 para un centro de datos individual y un pequeño número de bases de datos con un volumen de transacción "normal" que utilicen capacidades de monitoreo esenciales. Las instalaciones más grandes con impacto amplio (en términos geográficos y de volumen de base de datos/transacción) y funcionalidad añadida pueden costar $1 millón o más. El costo crece casi linealmente con los requerimientos, y las empresas típicamente empiezan con implantaciones de alcance limitado, para después aumentar a implantaciones más grandes después de 12 a 18 meses.

Proveedores de tecnología

- La suite DbProtect de **Application Security** combina el producto de monitoreo de la compañía con su herramienta de gestión de derechos de usuario y su producto de escaneo de vulnerabilidad líder en el Mercado. Application Security tapó un hueco de funcionalidad en 2011 añadiendo prevención a la suite. La compañía tiene una base fuertemente instalada por el lado de la vulnerabilidad y la ha usado en ventas de monitoreo.
- **BeyondTrust** adquirió las acciones de Lumigent, uno de los primeros proveedores de DAM y de los primeros líderes en el mercado. La oferta de Lumigent encaja bien con el portafolio de BeyondTrust, pero el desarrollo limitado del viejo producto de Lumigent ha resultado en algunos huecos de funcionalidad en su oferta. BeyondTrust ha tapado algunos de estos huecos con su último producto y se ha comprometido a abordar otros en futuros productos.
- **IBM InfoSphere Guardium** es el líder en el mercado en términos de ganancias y número de clientes. Su oferta tiene la cobertura de plataforma más amplia y el conjunto más robusto de características, y la compañía ha demostrado la capacidad para usar el modelo de ventas de IBM con su oferta de DAP.
- **Imperva** es segundo en el mercado de DAP, con alcances y ofertas similares a las de IBM. La compañía vende DAP como parte de una suite de seguridad de datos que incluye un firewall de red y un producto para seguridad de datos no estructurados.
- **McAfee** adquirió el producto DAM de Sentrigo y está empujando de manera importante en el mercado de seguridad de las bases de datos. Si McAfee puede utilizar su gran base de clientes y fuerza de ventas, entonces puede ser un fuerte competidor en este mercado.

- **Oracle** tiene una fuerte presencia en el mercado, especialmente entre su base de clientes. Oracle provee mucha funcionalidad DAP con dos productos separados: Audit Vault y Database Firewall, que proveen soporte para sistemas de gestión de base de datos Oracle y no Oracle. Oracle ofrece varias herramientas de distintas marcas que se corresponden con capacidades DAP extendidas, algunas de las cuales son multiplataforma y algunas de las cuales sólo tienen compatibilidad para RDBMSs de Oracle.
- **WareValley,** un proveedor surcoreano con fuerte enfoque y presencia en el mercado de Asia/Pacífico, tiene una oferta que consiste en encriptación, monitoreo, gestión de vulnerabilidad y gestión de RDBMS. La compañía ha mostrado recientemente un deseo creciente por moverse a los mercados de Norteamérica y la Unión Europea con precios agresivos.

Evidencia

Más de 100 encuestas a clientes han mostrado un conjunto de requerimientos cambiante — desplazándose del monitoreo más básico a necesidades más avanzadas como el descubrimiento, la prevención y la gestión de vulnerabilidad. Las sesiones informativas de los proveedores y otras discusiones con ellos han mostrado agresivos planes de acción con capacidades expandidas en el corto, mediano y largo plazo.